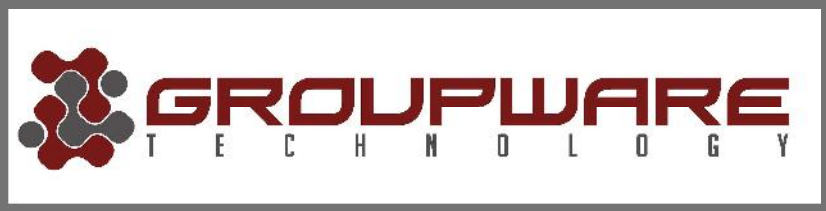


Advanced IPv6 Design and Deployment for Enterprise Networks with Microsoft Windows™ Technology

Presentation Handout

Version 1.0

January 3rd, 2012

TABLE OF CONTENTS

ASSUMPTIONS OF IPV6 KNOWLEDGE FOR WINDOWS 4

SECTION A – INTERNET EDGE 7

Dual Stack your Internet Edge 7

Basic IPv6 Internet Edge Key Items 7

IPv6 Internet Edge Caveats 7

SECTION B - DIRECTACCESS 8

IPv6 Requirements with DirectAccess 8

DirectAccess Key Items 8

SECTION C - FIREWALLS 9

Dual Stack your Firewalls 9

Basic IPv6 Firewall Items 9

IPv6 Firewall Caveats 9

SECTION D – APPLICATION DELIVERY CONTROLLERS 10

Basic ADC IPv6 Requirements 10

ADC IPv6 Caveats 10

SECTION E – MICROSOFT EXCHANGE IN THE DMZ 11

Microsoft Exchange Edge Transport and IPv6 11

Basic Microsoft Exchange IPv6 Requirements 11

Microsoft Exchange Edge Transport and IPv6 Caveats 11

SECTION F – MICROSOFT EXCHANGE 13

Microsoft Exchange and IPv6 13

Basic Microsoft Exchange IPv6 Requirements 13

Microsoft Exchange and IPv6 Caveats 14

SECTION G – MICROSOFT FILE AND PRINT 15

Microsoft File and Print and IPv6 15

Basic Microsoft File and Print IPv6 Requirements 15

File and Print IPv6 Caveats 15

SECTION H – MICROSOFT ACTIVE DIRECTORY AND GROUP POLICY 16

Microsoft Active Directory and IPv6 16

Microsoft Active Directory and IPv6 Key Items 16

Microsoft Group Policy and IPv6 16

SECTION I – MICROSOFT SHAREPOINT AND IIS 17

Microsoft SharePoint and IPv6 17

Microsoft IIS and IPv6 17

SECTION J – MICROSOFT WINDOWS CLIENT 18

Microsoft Windows Client and IPv6 18

Microsoft Windows Client IPv6 Items 18

Microsoft Windows Client IPv6 Caveats 18

SECTION K – WAN 20

WAN and IPv6 20

SECTION L – REMOTE OFFICE 21

Remote Office and IPv6 21

SECTION M – ADDITIONAL REFERENCE MATERIAL 22

RFC's 22

Ipv6-literal.net Names 22

Link-local Multicast Name Resolution 22

Recommended reading 22

COPYRIGHT AND TRADEMARK 24

PRESENTATION HANDOUT FOR

Advanced IPv6 Design and Deployment for Enterprise Networks with Microsoft Windows Technology

Assumptions of IPv6 Knowledge for Windows

The presentation that corresponds with this document makes the following assumptions in the audience knowledge base.

- Previously done IPv4 Design and Deployment of Microsoft technologies
- Designed and Deployed IPv4 DHCP and DNS
- Understands basic IPv4 routing, subnetting and routing protocol behavior
- Has utilized the Infrastructure Planning and Design (IPD) Guides from Microsoft to Deploy Exchange, SharePoint, Active Directory, File Services, Print and other technologies
- Has a working knowledge of IPv6, addresses, subnetting and routing

Information about IPD's can be found at:

http://technet.microsoft.com/en-us/library/cc196387.aspx

It is important to know that the TCP/IP protocol stack in Windows Server 8, Windows Server 2008 R2, Windows Server 2008, Windows 8, Windows 7, and Windows Vista is a dual IP layer implementation. This is different than older version of Windows and is also different than how other OS manufactures implement IPv6. The following diagram is from Understanding IPv6, 2nd Edition by Joseph Davies, Microsoft Press.

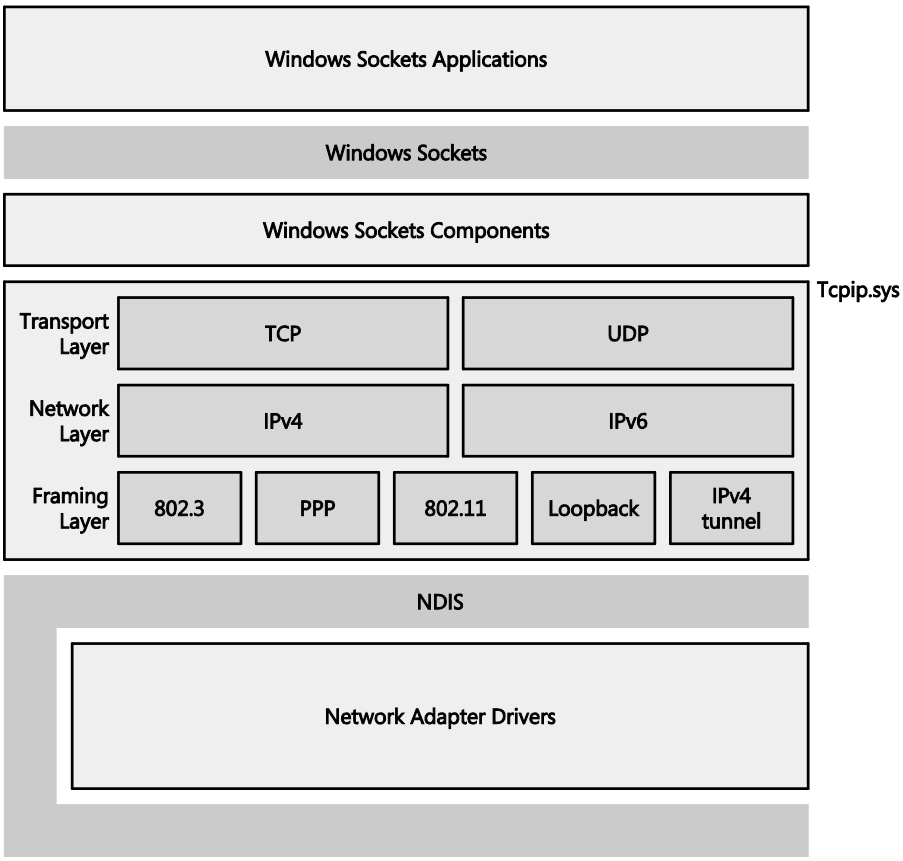


Figure 1-1 The architecture of the TCP/IP protocols for Windows

Each section below corresponds to the appropriate labeled section of the main presentation overview diagram. The diagram is the reference point architecture and the sections address IPv6 design and deployment considerations for each section.

The following diagram showing each sections representation in a typical Enterprise network deployment:

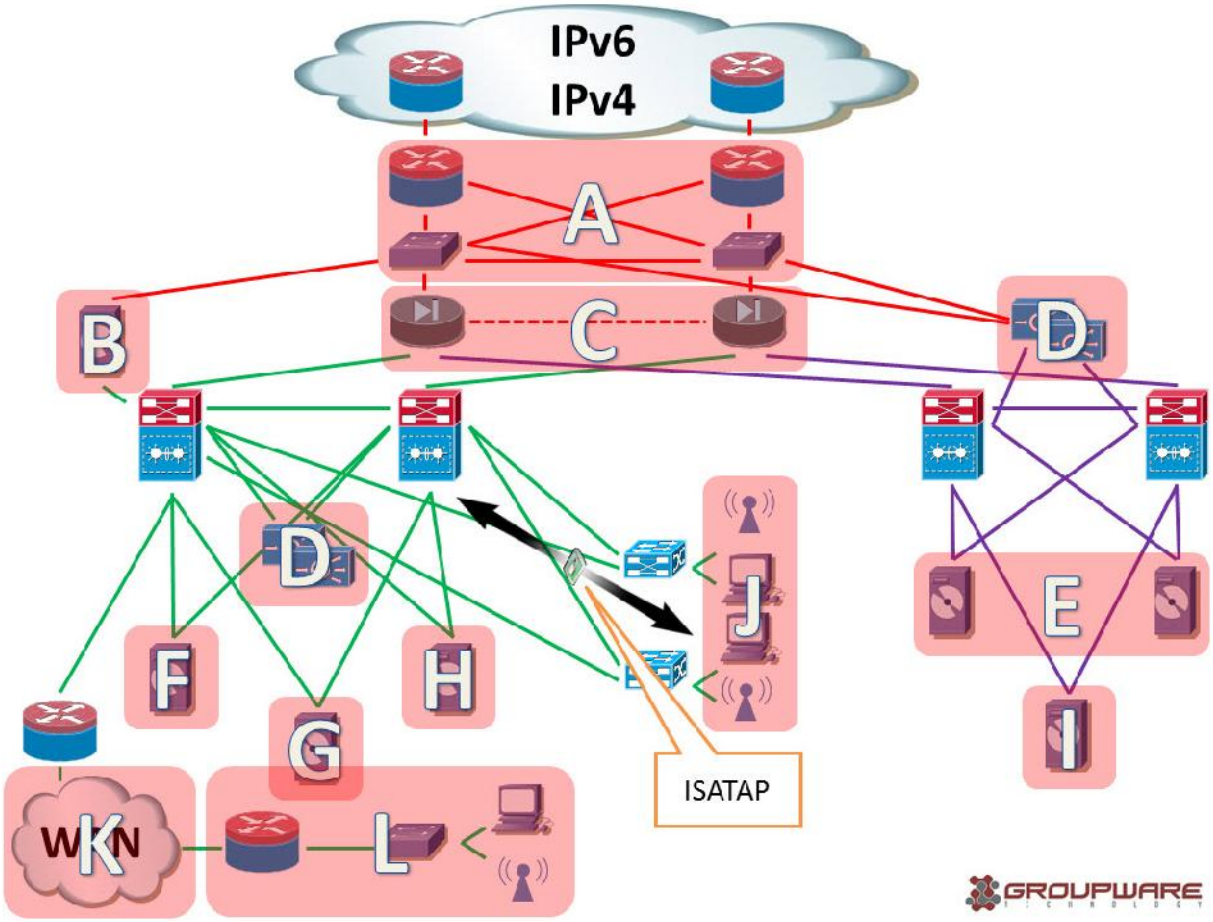


Figure 1-2 Typical Enterprise Network Topology with Sections labeled

Section A – Internet Edge

Dual Stack your Internet Edge

The Internet Edge design should assume full dual stack support and upgrading equipment to be able to do this function is important. While there are transition solutions available to enable web, mail and DNS content to be translated the most efficient process is to get your Internet routers, switches and firewalls working with IPv6 in addition to IPv4.

Basic IPv6 Internet Edge Key Items

For Enterprise deployments typically a network team is responsible for Internet Edge access for IPv4 however for Commercial and SMB it is very common for system administrators to also design, deploy and operationally maintain this area. The key items for the Internet Edge when bringing up IPv6 would be:

- Prefer native IPv6 BGP peering if the solution is multihomed
- Do not rely of IPv4 BGP peering for IPv6 BGP – run separate BGP IPv4 and IPv6 neighbor configurations for each protocol per service provider link
- Obtain the same SLA for IPv6 as you have for IPv4
- Ensure you are advertising the correct IPv6 prefix to each peer
- Register your IPv6 prefix in the appropriate routing registry
- Apply appropriate ingress and egress filters for IPv6 prefixes (only take inboud traffic destined for your prefix, only allow your prefix outbound)
- Ensure you have enough CPU and Memory to handle IPv6 routing table growth
- In simpler edge deployments utilize static routing
- Statically assign IPv6 addresses for firewalls, routers and loopbacks
- Ensure you have DNS entries (forward and reverse) set up for your edge devices
- Set up support for ipv6-literal.net DNS names for edge devices in case DNS is not available
- Turn on RA-Guard and/or MAC filters on edge ports to reduce default gateway errors

IPv6 Internet Edge Caveats

Often it is not possible to get native IPv6 service from Internet Service Providers (ISP) today. If it is not possible to have native IPv6 service then a tunnel solution across IPv4 may be your only option until native IPv6 service is available. If that is the case consider the following:

- Utilize Hurricane Electric's tunnel broker services – they will do BGP peering and allow you to advertise your IPv6 prefix through them – http://www.tunnelbroker.net/
- Do NOT deploy 6to4 at your Internet Edge and run public IPv6 services with 6to4 addresses
- If you cannot utilize a tunnel service, look at other service providers to obtain IPv6 native peering
- If you are unable to turn up a proper IPv6 Internet Edge solution do NOT turn on your internal access (client) ports with that IPv6 prefix as you will break your client OS and Internet access
- Do not use ULA on the Internet Edge at all and do not advertise ULA addresses externally

Section B - DirectAccess

IPv6 Requirements with DirectAccess

DirectAccess (DA) is an enhanced VPN solution from Microsoft that allows Windows 7 and Windows 8 domain joined clients to be always on and connected to their Enterprise network in a secure and seamless way. The IPv6 protocol for Windows is a requirement for DirectAccess deployment.

Some of the new enhancements in Windows Server 8-based DirectAccess is that the server uses NAT64/DNS64 to allow DirectAccess clients (IPv6-only nodes) access to intranet servers and resources that are only available over IPv4. This reduces the overall footprint requirement of IPv6 support on the internal network however do realize the clients are still IPv6 only nodes on the network and will NOT have an IPv4 internal address.

For Windows Server 2008R2 DirectAccess solution no NAT64/DNS64 solution is available natively in the server platform unless the solution is deployed using Forefront UAG (Unified Access Gateway) Because of this, current DirectAccess solutions REQUIRE IPv6 support in the internal network. This can be accomplished utilizing one of the following solutions:

- ISATAP – to allow the IPv6 only clients access to the resources they require on the intranet ISATAP can be deployed for devices they need to reach. Not all Windows Servers would be required to participate in the ISATAP configuration but at a minimum a domain controller, DNS server, Exchange Server CAS and UM and/or Lync Server and likely a file and printer server and SharePoint would need to be configured.
- Dual stack native IPv6 solution to allow the clients to reach all IPv6 enabled servers and clients on the internal network
- SLB64 solution if only web and DNS solutions would be required – this would be a very restrictive deployment of DirectAccess and is not recommended unless it meets a specific use case

DirectAccess Key Items

The key items for DirectAccess are:

- IPv6 is required for DA clients
- DA clients can only be Windows 7 and Windows 8
- If DA clients want to access an intranet resource it will need to do so utilizing IPv6 or have a transition solution in place
- The easiest way to deploy DA today (pre Windows Server 8) is to utilize Forefront UAG which has transition solutions in place
- For a Proof of Concept (POC) it is fine to utilize ISATAP however for a production deployment do not utilize ISATAP
- For production DA, enable dual stack IPv6 to avoid issue with troubleshooting ISATAP tunnel problems
- If you must deploy DA with ISATAP set up a Service Block IPv6 Solution to terminate all the ISATAP tunnels in a common area, it will reduce errors and ease troubleshooting
- DA server and clients must be able to communicate with an AD server for authentication so a minimum of one AD server must be dual stacked

For more information, see the IPD for DirectAccess.

Section C - Firewalls

Dual Stack your Firewalls

If you existing firewall does not support IPv6 there is no way for you to control IPv6 traffic from the Internet Edge to the inside of your network. This is a fundamental problem that cannot be overcome with any transition solution available today.

It is possible to bypass your IPv4 firewall and simply route via a tunnel all external IPv6 traffic to an internal IPv6 router but this removes all centralized ingress and egress firewall policies and is not recommended. Instead, obtain a dual stack firewall solution.

Basic IPv6 Firewall Items

For Enterprise deployments typically a network or security team is responsible for firewall policies and enforcement however for Commercial and SMB it is very common for system administrators to also design, deploy and operationally maintain these devices. The key items for firewalls when bringing up IPv6 would be:

- Do not try and duplicate ALL your IPv4 rules to IPv6
- You will need new ICMPv6 rules that are different then your IPv4 ICMP rules
- Only port over specific IPv4 rules to IPv6 IF the service is running on IPv6 also
- Because the firewall will be routing IPv6 prefixes your rules should be based on either static IPv6 host addresses or /64 prefixes, in some cases it may be for larger prefixes (site wide rules)
- If you have a native dual stack solution running block tunneling and transition technologies for IPv6
- Utilize local server and client host firewalls to help protect devices when doing initial IPv6 turn up and deployment
- Utilize IPS and IDS systems that are IPv6 aware and can perform inspection and matching in tunnels for IPv6

IPv6 Firewall Caveats

Firewall functions will differ between IPv4 and IPv6. Primarily they will provide IP and port ingress and egress access control but often IPv4 firewalls also provide both NAT and PAT functions. Because IPv6 does not have equivalent NAT and PAT functions (only Prefix translation – see RFC 6296) it logically makes sense that the firewall will not do this. While this simplifies the definition of an end host and should in theory make firewall policy management easier there are problems with correlating the IPv4 address with its dual stack IPv6 address. To overcome some of these limitation there are some interesting options of embedding IPv4 addresses into IPv6 to allow correlation and tracking. These discussions are outside of the scope of this document but may be addressed in future updates.

Not all firewall manufactures are supporting IPv6 natively today. Microsoft's commercial firewall product is Forefront TMG and unfortunately at this time TMG does not support native IPv6 at all. This means you either need to install separate IPv6 firewalls for the purpose of doing IPv6 traffic or you migrate to a new firewall product. Current common industry standard firewalls that do support IPv6 are Cisco ASA, Juniper SRX & ISG, Sonicwall, Fortinet, Palo Alto Networks and Checkpoint (this is not a complete list by any means.)

Client operating systems today by default have firewalls enabled. All Windows 7 and Windows 8 OS platforms do this by default and will perform firewall functions for both IPv4 and IPv6. Rules for the advanced firewall can be configured via Group Policy, GUI or PowerShell. In addition, a host firewall for Windows Server 2008 R2 and Windows Server 8 can be enabled and similar GP, GUI or PowerShell functions can be employed to manage those platforms as well. The advanced firewall on both client and server also manage the IPsec VPN configuration for both IPv4 and IPv6.

Section D – Application Delivery Controllers

Basic ADC IPv6 Requirements

One of the unique capabilities of ADC's (also referred to as Server Load Balancers or SLB's) is that they can be utilized to translate between IPv4 and IPv6. Because of this basic property they become very strategic in solving specific IPv6 use case scenarios such as:

- IPv6 Internet Edge is working but no Enterprise DMZ applications such as web, DNS or mail services are dual stacked yet
- IPv6 clients are working but no other intranet application services are IPv6 enabled
- IPv6 clients are working but need to access IPv4 Internet

Because the ADC has both a native IPv6 and IPv4 address (dual stacked) it is able to translate and proxy services in either direction depending on the need requirements. ADC's in their traditional role allow public virtual IP addresses to be load balanced and/or policy routed to real IP addresses on the intranet. This specific function can happen in the following scenarios:

- IPv6 VIP addresses to IPv6 real server addresses
- IPv6 VIP addresses to IPv4 real server addresses
- IPv4 VIP addresses to IPv6 real server addresses
- IPv4 VIP addresses to IPv4 real server addresses

An additional function is the ability to work with a device that can perform DNS64 (build synthetic IPv6 AAAA records from only an IPv4 A records) for IPv6 only clients and then map that to the NAT64 function in the ADC device. ADC's can be used to perform global load balancing via DNS manipulations and other unique application services but those are outside the scope of this handout.

ADC IPv6 Caveats

ADC's do have some IPv6 specific issues to worry about:

- DNS64/NAT64 does not support DNSSEC
- ADC's do not provide any applications specific IPv6/IPv4 proxy services outside of web, DNS and basic TCP services – more sophisticated services are coming out or are road mapped
- The ADC's can become a single bottleneck of traffic congestion if all IPv6/IPv4 traffic is moving through the device in an Enterprise application solution
- ADC's can complicate troubleshooting application problems
- Most ADC's today do not have prefix translation as a feature

For more information about ADC's recent performance and functions around IPv6 see Scott Hogg's Network World article at: http://www.networkworld.com/reviews/2012/021312-ipv6-application-delivery-controllers-side-255478.html

Section E – Microsoft Exchange in the DMZ

Microsoft Exchange Edge Transport and IPv6

One of the most commonly deployed Microsoft products is Exchange. Exchange 2010 has some specific roles in its recommended deployment topology that need to be addressed when utilizing IPv6.

This section covers the specific Exchange 2010 role of Edge Transport and its deployment in an Enterprise DMZ or Internet Edge environments. This role may be affected by IPv6 in hybrid cloud hosting solutions depending on if a PaaS or IaaS environment is selected.

Basic Microsoft Exchange IPv6 Requirements

Microsoft Exchange relies on IPv6 for connectivity between hosts if the Exchange servers are able to communicate with IPv6 link local addresses or Global Unicast Addresses and resolve host names with AAAA records. It is important for Exchange administrators to realize that when deploying highly available Microsoft Exchange solutions within the same vlan or subnet that their Exchange servers will prefer to use IPv6 to do all host to host communications and will prefer to do so utilizing link local addresses.

In addition, if Unique Local Addresses (ULA) or Global Unicast Addresses (GUA) are used in the deployment and AAAA host records are available for all Exchange servers within the environment that IPv6 will also be the preferred method of host to host communication across layer 3 boundaries.

If an Exchange server performing the Edge Transport role performs an external DNS lookup and resolves an MX record to an IPv6 addresses and it has a native IPv6 or transition technology IPv6 address it will first attempt to communicate using IPv6.

Now that we understand this basic behavior (that when available IPv6 is always used first) what happens when IPv6 is broken in some way to the remote host you are trying to communicate with? Windows Server 2008 R2 OS's networking stack will do in summary the following (based on RFC3484 – see the RFC for specific behavior – this is a summary):

- If a DNS query returns an AAAA and an A record the IPv6 address will be utilized first for the session attempt, this includes all transition and tunneling technology IPv6 solutions except Teredo (there is a specific order of operation is there is more than one IPv6 address on the host)
- After attempting to connect via IPv6 to the remote host and failing for a standard default timeout of "X" minutes the host will then attempt to connect utilizing IPv4 via the A record provided
- If no A record is returned via DNS then the host session timeout will occur and the host will give up attempting to connect to the remote resource until the application requests a session again

What impact does this have on Exchange depends on the service role Exchange is providing. In an Edge Transport role in the DMZ where communications is SMTP then Exchange will do slightly more sophisticated default behavior. Exchange will attempt to connect with IPv6 if an MX record has an IPv6 entry available. A key difference is that if the Exchange Edge Transport server is in a DMZ with public IPv4 addresses prior to attempting to deliver via IPv4 it will attempt to utilize a 6to4 transition technology to see if it can deliver SMTP mail via that method. If ISATAP is enabled in the DMZ the Exchange server will then attempt to use the ISATAP tunnel prior to 6to4. If Exchange is unable to connect to the host via IPv6 it will immediately attempt to connect to the IPv4 address in the MX record if it is available to deliver SMTP mail.

Microsoft Exchange Edge Transport and IPv6 Caveats

One key critical items often forgotten for Exchange Edge Transport role is for system administrators to turn off all the IPv6 transitions technology solutions on the server, regardless of if dual stack is enabled or not. This recommendation is not in the Exchange IPD but I recommend it be done to avoid the following issues:

- If a DNS query returns an AAAA and an A record the IPv6 AAAA record will be utilized first for the session attempt, this includes all transition and tunneling technology IPv6 solutions except Teredo
- If 6to4 is utilized because the Exchange server has a public IPv4 address it will attempt to deliver using IPv6 with that address but a firewall or public Internet routing problems could break 6to4 and therefore break Exchange. This introduces higher latency to get SMTP traffic to the end destination
- Eases the troubleshooting process for IPv6 connectivity and when things are broken

The reason this is commonly overlooked is that many system administrator fail to remember that transitions services are enabled by default in non-domain joined servers. The IPD recommends that the Edge Transport role either be standalone workgroup mode or a separate domain be put in place specifically for those servers. Most Enterprise deployments I have seen elect to do a workgroup solution, hence the transition technologies are on by default.

There are legitimate reasons to leave the transition services enabled, just document and define the use case you have for having it on.

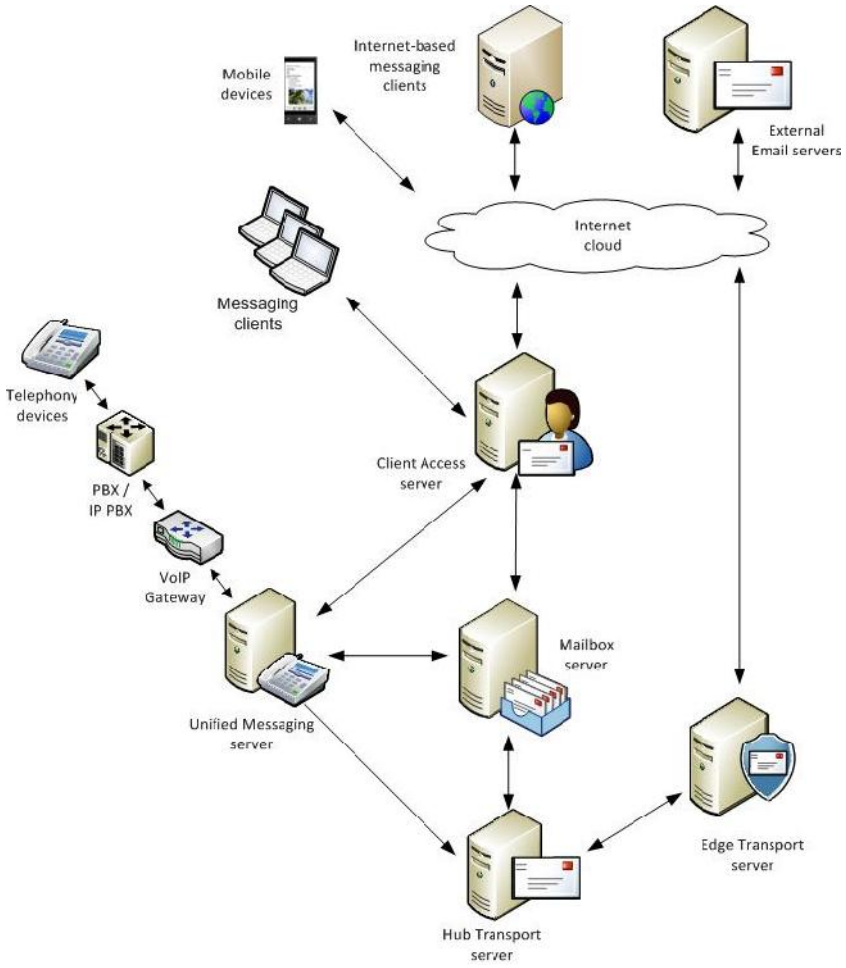
Section F – Microsoft Exchange

Microsoft Exchange and IPv6

One of the most commonly deployed Microsoft products is Exchange. Exchange 2010 has some specific roles in its recommended deployment topology that need to be addressed when utilizing IPv6.

This section covers the specific Exchange 2010 roles of Client Access Server (CAS), Hub Transport, UM and its deployment in an Enterprise environments. This role may be affected by IPv6 in hybrid cloud hosting solutions depending on if a PaaS or IaaS environment is selected.

The following graphic is from the Exchange 2010 SP1 IPD published by Microsoft:



Basic Microsoft Exchange IPv6 Requirements

Microsoft Exchange relies on IPv6 for connectivity between hosts if the Exchange servers are able to communicate with IPv6 link local addresses or Global Unicast Addresses and resolve host names with AAAA records.

This behavior holds true for all the Exchange server roles for 2010, specifically Unified Messaging, Hub Transport and Client Access.

All the same IPv6 requirements of the Edge Transport role apply to the other roles however they are typically not deployed in environments that could potentially utilize public IPv4 addresses. Please refer to the previous section for Microsoft Exchange IPv6 requirements.

Microsoft Exchange and IPv6 Caveats

One key critical items often forgotten for Exchange 2010 roles is for system administrators to turn off all the IPv6 transitions technology solutions on the server. This recommendation is not in the Exchange IPD but I recommend it be done to avoid the following issues:

- If a DNS query returns an AAAA and an A record the IPv6 AAAA record will be utilized first for the session attempt, this includes all transition and tunneling technology IPv6 solutions except Teredo
- If 6to4 is utilized because the Exchange server has a public IPv4 address it will attempt to deliver using IPv6 with that address but a firewall or public Internet routing problems could break 6to4 and therefore break Exchange. This introduces higher latency to get SMTP traffic to the end destination
- Eases the troubleshooting process for IPv6 connectivity and when things are broken

Turning off the transition solutions on these Exchange roles can be handled via Group Policy in Active Directory. Additionally, transition solutions are not recommended unless you have specifically designed to utilize them. To see more information about how to use Group Policy to set 6to4, ISATAP, Teredo and IP-HTTPS see:

http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx

Section G – Microsoft File and Print

Microsoft File and Print and IPv6

Microsoft Windows Server 2008 R2 (and soon Server 8) is often used for file and print services within Enterprise, Commercial and SMB entities to allow their employees to access files and to print information required to perform their job function. It is important that these servers have IPv6 available to allow IPv6 client devices to be able to access them natively.

Basic Microsoft File and Print IPv6 Requirements

Microsoft Windows Server 2008 R2 (and soon Server 8) are all capable of supporting IPv6 natively and are also able to provide some proxy like functions for file and print. Specifically, if the servers are dual stacked then a request to print something from a client can be put in the print queue and even though the printer may only support IPv4 it is possible for the server to still provide print jobs to that printer via IPv4 communication.

The same holds true for file storage. A client that is communicating with the server via IPv6 will have no issues nor will and IPv4 client that is communicating to the same server to access the same file. If the two clients are attempting to directly communicate but do NOT have a common protocol (IPv4 or IPv6 in common)they will be unable to access the file from the other device. This would more commonly happen in workgroup or peer to peer configurations.

BranchCache is fully able to utilize IPv6 to optimize file usage across branch office locations. More details about BranchCache can be found at:

http://technet.microsoft.com/en-us/network/dd425028

File and Print IPv6 Caveats

Microsoft Windows Server 2008 R2 (and soon Server 8) are able to communicate with IPv6 to printers however many older printers will not support IPv6. This is why it is critical that the servers be dual stacked and have IPv4 access so they can communicate with older printers whose life cycle has not yet been reached. Additionally, newer printers that do support DHCPv6 should have a DHCPv6 reservations (M bit set) so they have a well-known IPv6 addresses or have static IPv6 addresses with appropriate DNS AAAA records. Printers should NOT make use of SLAAC nor Stateless DHCPv6 (O bit set) unless there is a specific use case for that, perhaps in a guest network.

Shared file storage should be accessible via IPv4 or IPv6 if the sever is dual stacked. For UNC share names if no IPv6 AAAA record is available for hostname resolution and Link-local Multicast Name Resolution (LLMNR) is not available because the client and server are not on the same subnet then IPv6 literal names must be used to access the share. This is true for other Microsoft services that make use of UNC. The reference section has information about IPv6 literal names and LLMNR.

BranchCache can have limitations if remote site clients are a mix of IPv4 only and IPv6 only. Specifically, in the deployment case where Distributed Cache mode is used clients may be unable to connect to each other if they are not utilizing the same IP protocol version. This would cause duplicate file caching on IPv4 hosts vs. IPv6 hosts. This is not an issue for Hosted Cache mode if the server is dual stacked.

Section H – Microsoft Active Directory and Group Policy

Microsoft Active Directory and IPv6

Since Windows Server 2008 IPv6 has been enabled and used by default. In addition to it being enabled the entire OS and its associated core functions were rewritten to fully support IPv6. This meant that basic items like all fields that took IP addresses had to accept both IPv4 and IPv6. It also meant that because IPv6 was used first for sessions between hosts that all higher application services had to support IPv6. Since Windows OS utilizes Winsock and other standardized API's and drivers developed by Microsoft it was logical that one of the key services that Windows provides, Active Directory (AD), would fully use IPv6 and have IPv6 information stored in it.

Microsoft Active Directory and IPv6 Key Items

If hosts running AD have transport available between them utilizing IPv6 they will perform all their functions like replication, authentications, and authorization over that IPv6 transport. Some key requirements that are forgotten by system administrators when IPv6 is deployed throughout a network is simple upkeep. Adding the appropriate IPv6 /64 subnets to Sites and Services/Sites/Subnets so that replication flow matches what you originally designed for IPv4.

More information about Sites and Services/Sites/Subnets can be found at:

http://technet.microsoft.com/en-us/library/cc740187%28v=ws.10%29.aspx

The good news is that Exchange will leverage the work you perform in Sites and Services in addition to the mail routing policies you set up depending on how complex your Exchange deployment is this can be critical to ensuring that the Exchange servers are forwarding authentication request to the correct domain controller.

Microsoft Group Policy and IPv6

The Group Policy function within AD leverages the transport selection that AD uses to replication and push out policy configurations throughout the network. One of the challenges is that Group Policy Objects (GPOs) can only be pushed to hosts that are able to connect to their appropriate AD domain controller server. This means it is critical that the server be dual stacked so that GPOs can be pushed to older platforms that may not support IPv6. Also, for specific use cases where clients are IPv6 only (such as DA clients) the server must be able to provide the GPOs over IPv6.

There are many IPv6 specific GPO's available to control hosts behavior unfortunately all the sites that document them are for the purpose of disabling IPv6! Microsoft has stated explicitly that they do NOT recommend disabling IPv6 at all and that often doing so will break some application functionality. With that being said, here is a link on IPv6 registry keys and GPOs:

http://support.microsoft.com/kb/929852

Section I – Microsoft SharePoint and IIS

Microsoft SharePoint and IPv6

Microsoft Windows Server 2008 R2 and soon Windows Server 8 have full support for IPv6. Microsoft SharePoint relies on Internet Information Server (IIS) to run the web front end service. Because IIS has full IPv6 capabilities SharePoint also has IPv6 capabilities. IIS is able to run web services simultaneously on IPv4 and IPv6 and it is recommended that the server be dual stacked.

SharePoint also relies on SQL Server and if SQL is installed on a remote host it will use IPv6 as its primary transport if IPv6 is available. Because SharePoint may make use of UNC path information it is critical that proper DNS be in place so that IPv6 literals do not have to be used. SharePoint also relies of AD for user authentication and that too will happen over IPv6. There may be cases where webparts or externally imbedded context is available over IPv4 only. It is important for the SharePoint server to be dual stacked to be able to support pulling that content. Also, clients that are connecting to the dual stack server should be dual stacked themselves if external content is rendered and are provided through both IPv4 and IPv6 otherwise content may not render correctly.

This situation can easily be tested by setting up IPv4 only and IPv6 only clients and connecting to the SharePoint site. If content is missing on the page then likely a content part is only available over one protocol.

Microsoft IIS and IPv6

Microsoft IIS has other functions besides providing web content or the front end function for SharePoint. It is also used by Microsoft Exchange for the CAS role, by AD for the Certificate Server role and by other Microsoft products. In the specific case of Certificate services IIS is able to appropriately issue certificates with IPv6 address information, provide CA and CRL services via IPv6 and perform authentications against AD via IPv6.

In the Microsoft Exchange CAS role it is able to provide the front end web, ssl, active sync and other services via IPv6 in addition to IPv4. Because Microsoft is now recommending ADC's instead of Microsoft's native NLB for the CAS role IPv6 to IPv6 ADC functions are critical for IPv6 or dual stack deployments.

Section J – Microsoft Windows Client

Microsoft Windows Client and IPv6

Since Microsoft release Windows Vista on January 30th, 2007 IPv6 has been part of the Windows Client. For earlier Windows Clients, specifically Windows XP there was an option to add IPv6 to the client OS however while the implementation works it is no longer RFC standards compliant and is not considered a supportable IPv6 client OS. In addition, on April 8th, 2014 Windows XP will no longer be a supported OS. This document is focused around Windows Clients from Windows Vista on. It assumes that Enterprises that still have large install bases of Windows XP will NOT deploy IPv6 for those devices and will not install the IPv6 add on for that client due to its shortcomings in proper IPv6 support.

In addition to IPv6 Microsoft included transition technologies in the client, specifically ISATAP, 6to4 and Teredo. These transition technologies are enabled and on by default for 6to4 (if the host has a public IPv4 address) and for ISATAP if the appropriate ISATAP prefix is available via DNS. Teredo is enabled but not on by default though any applications that make an appropriate API call can turn it on assuming it is not explicitly disabled.

Microsoft Windows Client IPv6 Items

Microsoft Windows Vista, Windows 7 and soon Windows 8 are all capable of supporting IPv6 natively. Because IPv6 is on by default and utilized first for all session requests if a AAAA record is provided via DNS it is important to understand that while native IPv6 will be used first if a transition technology is enabled and able to function (or appears to function) it will be utilized next. Transition technologies are used first if no native IPv6 is available on the client. This may not seem intuitive since the client will require IPv4 in order to make use of the transition technology.

Because of this behavior there are use cases where having poor performing native or transition technologies via IPv6 will detrimentally impact the end user experience. It is also possible for the client to have poor performance time in failing from IPv6 back to IPv4 in things like web browsing or file share access. These latency problems are difficult for help desk to troubleshoot and most often result in complaints of "network is slow."

Recently some newer methods have been introduced to try and address this problem. Specifically RFC 6555 or Happy Eyeballs. In summary, the RFC talks about either applications or operating systems implementing session requests simultaneously via IPv4 and IPv6 and then using an algorithm to determine which protocol session to use and how often to periodically retest. At this time, Windows Vista and Windows 7 do not have support for RFC 6555 nor does Internet Explorer 9 (IE 9) and it is unlikely they will have supported added. Microsoft has not released a public statement of roadmap or support for RFC 6555 for Windows 8 or Internet Explorer 10 (IE 10).

Assuming RFC 6555 support makes it into Windows 8 at the operating system level then all applications would benefit from this OS behavior. If, alternatively they only enable it in Internet Explorer 10 then only applications that rely on IE 10 and IE10 itself would benefit from this feature. It would seem a more desirable function to have in the OS and it is my hope that is how Microsoft implements it if they chose to do so.

Microsoft Windows Client IPv6 Caveats

Microsoft Windows XP should not be utilized or deployed with IPv6 at all. While it is still the most widely deployed Windows client to date, Enterprises, Commercial, and SMB's should have begun the deployment stages of Windows 7 already. The timing of the Windows 7 client deployment may shape the timing and execution of IPv6 at the access layer but there is no reason that the core, dmz, Internet edge and server platforms could not be dual stacked while waiting for the client devices to be upgraded.

There are situations where embedded devices or mobile platforms might never support IPv6 due to limitations of the hardware and the inability to upgrade to support a newer protocol. This is why it is critical to dual stack so that these devices are able to communicate with existing network resources without problem. As these devices are

replaced over time they remaining dwindling number of IPv4 only devices can be isolated within the network to allow better control and access of IPv4 resources. Additionally, IPv4 would only have to be enabled on hosts that those devices needed to communicate with. Long term, the goal is for those devices to go away completely and run an entirely native IPv6 network.

Section K – WAN

WAN and IPv6

For Microsoft Enterprise, Commercial and SMB solutions across WAN networks (MPLS, VPN, Frame Relay, etc.) there should be no specific IPv6 issues related to the OS outside of path MTU. Best practices for AD with Sites and Services/Sites/Subnets is necessary to have correct authentication and traffic paths matching your WAN topology.

There are challenges with WAN and IPv6 but are more commonly issues for network architects to deal with and not systems administrators. There may be some overlap with WAN acceleration however as long as they work properly with IPv6 there should be limited issues in working with Windows.

Section L – Remote Office

Remote Office and IPv6

Remote offices are a unique challenges in terms of redundancy and high availability and Microsoft has specific solutions designed to address these needs. Specifically, since remote offices can become cut off from corporate office resources due to WAN or other issues it is important they have basic functions like user authentication, file and print access and increasingly unified communications.

There are no specific remote office IPv6 issues in a dual stack environment however if ISATAP is utilized and is terminated at a service block location back at the corporate office or data center then IPv6 will fail. In addition, it is not uncommon for remote offices to have local Internet access to offload WAN costs or even to only have connectivity to the corporate office via VPN over Internet technology. In these cases, more address planning has to be done to determine the public IPv6 use cases. If a service provider is providing IPv6 addresses and the company also has provider independent space which is utilized at the remote office or are both utilized?

There might be a need to have a specific source address selection process but currently today there is not a good model in place to support propagating source address selection information from routing platforms down to hosts. Until that is solved dual homed non BGP peered configurations will have to utilize NPT66 (RFC 6296) in order to insure the correct prefix is utilized out of the right default gateway. NPT66 is not widely implemented in network devices today and until that is addressed more complex routing rules and interface preference setting may be required to have a solution that matches what IPv4 does today utilizing NAT.

Section M – Additional Reference Material

RFC's

The following RFC's related to IPv6 are referenced in this document:

- 2460 – IPv6
- 3068 - 6to4
- 3986 – URI Syntax
- 4193 – ULA
- 4380 – Teredo
- 5214 – ISATAP
- 6146 - NAT64
- 6147 - DNS64
- 6296 - NPT66
- 6343 - 6to4 advisory
- 6555 - Happy Eyeballs

Ipv6-literal.net Names

Windows supports the use of <ipv6 address>.ipv6-literal.net names. To specify an IPv6 address within the ipv6-literal.net domain name space, convert the colons (:) in the address to dashes (-). See http://msdn.microsoft.com/en-us/library/aa385353.aspx for specific details. In Windows you can use the ipv6-literal.net name in Uniform Naming Convention (UNC) path names. This is not to be confused with the URI IPv6 literal name path which uses the format of:

http://[ipv6 address]:<port number>

Link-local Multicast Name Resolution

The purpose of LLMNR is to allows hosts on the same subnet to be able to resolve hostnames without the need for a DNS server. It works over IPv4 and IPv6. With IPv6 it utilized a multicast process using FF02::1:3 and UDP port 5355. LLMNR is a Microsoft Windows specific technology. Other operating systems utilize different methods to perform local name resolution without DNS.

Recommended reading

Understanding IPv6 2nd Edition by Joseph Davies, Microsoft Press

IPv6 in Enterprise Networks by Shannon McFarland, Muninder Sambi, Nikhil Sharma, Sanjay Hooda, Cisco Press

IPv6 Security by Scott Hogg and Eric Vyncke, Cisco Press

Planning for IPv6 by Silvia Hagen, O'Reilly Press

IPv6 Essentials, 2nd Edition by Silva Hagen, O'Reilly Press

DNS and BIND on IPv6 by Cricket Liu, O'Reilly Press

Day One: Exploring IPv6 by Chris Grundermann, Juniper Networking Technologies Series

IPv6 Network Administration by Niall Richard Murphy and David Malone, O'Reilly Press

Running IPv6 by Iljitsch van Beijnum, Apress

Global IPv6 Strategies: From Business Analysis to Operational Planning by Patrick Grossetete, Ciprian Popoviciu, Fred Wettling, Cisco Press

Deploying IPv6 Networks by Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete, Cisco Press

Copyright and Trademark